PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-208406

(43)Date of publication of application : 25.07.2003

(51)Int.Cl. G06F 15/00
H04L 9/32

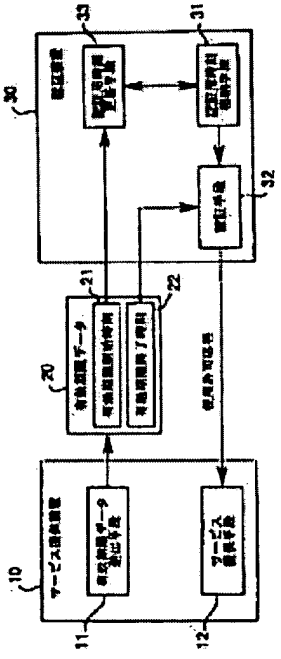
(21)Application number : 2002-334052

(22)Date of filing : 14.07.1997

(71)Applicant : FUJI XEROX CO LTD

(72)Inventor : KONO KENJI
TAGUCHI MASAHIRO
CHIBA KENJI

(54) SERVICE PROVIDING SYSTEM, AUTHENTICATION DEVICE, AND COMPUTER-READABLE RECORDING MEDIUM RECORDING AUTHENTICATION PROGRAM



(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal use by fabricating a set time of a service providing device in providing the online service with an appointed period.

SOLUTION: An effective time limit data sending means 11 of a service providing device 10 sends the effective time limit data 20 corresponding to a specific service to an authentication device 30. The authentication device 30 sends a use permission response to the service providing device 10 by an authentication means 32 when the authentication time is before the effective time limit termination time. An effective time limit starting time 21 is stored in an authentication time storing means 31 as a new authentication time in a case when the authentication time is before the effective time limit starting time 21. A service providing means 12 of the service providing device 10 provides the service to the user only when it receives the user permission response.

Japanese Laid-Open Patent Publication No.2003-208406 published on July 25, 2003. (partial English Translation)

【0051】

[S8] A decryption key decrypting part 203 decrypts an encrypted decryption key 315 by use of secret information 252 stored in PROM 250, and sends it back to the PC 110.

[S9] After receiving the decryption key, the PC 110 decrypts an encrypted software 320 on the basis of a command from a capsule activating program 311, and executes the software. At this time, the software 320 is not completely decrypted, instead, only one part to be executed is decrypted so as to be developed in the volatile memory. And then, the software decrypted and developed in the volatile memory is set to be deleted after the software is finished. Accordingly, there is no risk that the decrypted data is illegally used.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－208406
（P2003－208406A）
(43)公開日　平成15年７月25日(2003.7.25)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ　５Ｂ０８５
			３３０Ｂ　５Ｊ１０４
			３３０Ｇ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
			６７５Ｚ

審査請求　有　　請求項の数９　　ＯＬ　（全 16 頁）

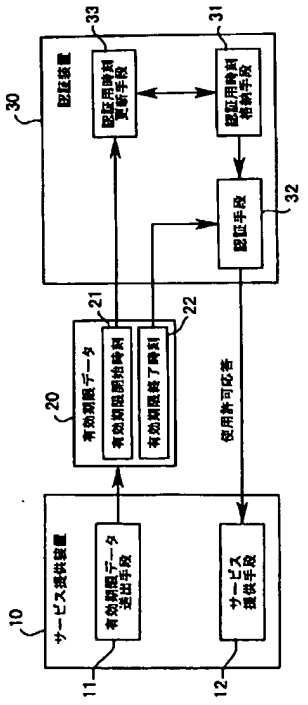
(21)出願番号　特願2002－334052(P2002－334052)
(62)分割の表示　特願平9－188246の分割
(22)出願日　平成９年７月14日(1997.7.14)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　河野　健二
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　田口　正弘
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　100092152
弁理士　服部　毅巖

最終頁に続く

(54)【発明の名称】　サービス提供システム、認証装置及び認証プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止できるようにする。
【解決手段】　サービス提供装置１０の有効期限データ送出手段１１が、特定のサービスに対応する有効期限データ２０を認証装置３０へ送出する。認証装置３０では、認証用時刻が有効期限終了時刻より前の時刻である場合には、認証手段３２により、使用許可応答がサービス提供装置１０へ送られる。また、認証用時刻が有効期限開始時刻２１より前の時刻である場合には、認証用時刻更新手段３３により、有効期限開始時刻２１が新たな認証用時刻として認証用時刻格納手段３１に格納される。サービス提供装置１０のサービス提供手段１２は、使用許可応答を受け取った場合にのみ、ユーザに対してサービスを提供する。



1

【特許請求の範囲】
【請求項１】　サービス提供装置と認証装置とから構成されるサービス提供システムであって、
前記サービス提供装置は、
特定のサービスに対応して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データを前記認証装置に出力する有効期限データ送出手段と、
前記認証装置から返された使用許可応答に基づいて前記特定のサービスを提供するサービス提供手段と、
を具備しており、
前記認証装置は、
認証用時刻を保持する認証用時刻格納手段と、
前記認証用時刻が前記サービス提供装置から受け取った前記有効期限データに含まれる前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
を具備していることを特徴とするサービス提供システム。
【請求項２】　サービス提供装置と認証装置とから構成されるサービス提供システムであって、
前記サービス提供装置は、
特定のサービスに対応して設定された有効期限開始時刻と有効期限終了時刻と該有効期限開始時刻および該有効期限終了時刻に対する署名とからなる有効期限データを前記認証装置に出力する有効期限データ送出手段と、
前記認証装置から返された使用許可応答に基づいて前記特定のサービスを提供するサービス提供手段と、
を具備しており、
前記認証装置は、
認証用時刻を保持する認証用時刻格納手段と、
前記サービス提供装置から受け取った前記有効期限データに含まれる前記署名に基づいて前記有効期限終了時刻が正しいことを確認した上で前記認証用時刻が前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
を具備していることを特徴とするサービス提供システム。
【請求項３】　サービス提供装置と認証装置とから構成されるサービス提供システムであって、
前記サービス提供装置は、
暗号化された特定のサービスに対応して設定された有効期限開始時刻、有効期限終了時刻、および該サービスの復号鍵が暗号化されたデータからなる認証データを前記認証装置に出力する認証データ送出手段と、
前記認証装置から返された前記復号鍵を含む使用許可応答に基づいて前記サービスを復号して提供することを可能とするサービス提供手段と、
を具備しており、
前記認証装置は、
認証用時刻を保持する認証用時刻格納手段と、
前記暗号化された復号鍵を復号する秘密情報を保持する秘密情報格納手段と、
前記認証用時刻が前記サービス提供装置から受け取った前記認証データに含まれる前記有効期限終了時刻より前の時刻である場合、前記秘密情報で前記復号鍵を復号し、復号された該復号鍵を含む前記使用許可応答を前記サービス提供装置に対して出力する認証手段と、
前記認証用時刻が前記認証データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
を具備していることを特徴とするサービス提供システム。
【請求項４】　サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データに基づいて該サービスの使用権の認証を行う認証装置であって、
認証用時刻を保持する認証用時刻格納手段と、
前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
を有することを特徴とする認証装置。
【請求項５】　サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と、該有効期限開始時刻および該有効期限終了時刻に対する署名からなる有効期限データに基づいて該サービスの使用権の認証を行う認証装置であって、
認証用時刻を保持する認証用時刻格納手段と、
前記サービス提供装置から出力された前記有効期限データに含まれる前記署名に基づいて前記有効期限終了時刻が正しいことを確認した上で前記認証用時刻が前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時

刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
を有することを特徴とする認証装置。
【請求項６】　サービス提供装置から出力される暗号化された特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と該暗号化されたサービスの復号鍵が暗号化されたデータとからなる認証データに基づいて該サービスの使用権の認証を行う認証装置であって、
認証用時刻を保持する認証用時刻格納手段と、
前記暗号化された復号鍵を復号する秘密情報を保持する秘密情報格納手段と、
前記認証用時刻が前記サービス提供装置から出力された前記認証データに含まれる前記有効期限終了時刻より前の時刻である場合、前記秘密情報で前記復号鍵を復号し、復号された該復号鍵を含む前記使用許可応答を前記サービス提供装置に対して出力する認証手段と、
前記認証用時刻が前記認証データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
を有することを特徴とする認証装置。
【請求項７】　サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
認証用時刻を保持する認証用時刻格納手段と、
前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に変更する認証用時刻更新手段と、
してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項８】　サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と該有効期限開始時刻および該有効期限終了時刻に対する署名からなる有効期限データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
認証用時刻を保持する認証用時刻格納手段と、
前記サービス提供装置から出力された前記有効期限データに含まれる前記署名に基づいて前記有効期限終了時刻が正しいことを確認した上で前記認証用時刻が前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項９】　サービス提供装置から出力される暗号化された特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と該暗号化されたサービスの復号鍵が暗号化されたデータとからなる認証データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
認証用時刻を保持する認証用時刻格納手段と、
前記暗号化された復号鍵を復号する秘密情報を保持する秘密情報格納手段と、
前記認証用時刻が前記サービス提供装置から出力された前記認証データに含まれる前記有効期限終了時刻より前の時刻である場合、前記秘密情報で前記復号鍵を復号し、復号された該復号鍵を含む前記使用許可応答を前記サービス提供装置に対して出力する認証手段と、
前記認証用時刻が前記認証データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、
してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はサービス提供システム、認証装置及び認証プログラムを記録したコンピュータ読み取り可能な媒体に関し、特に使用権の有効性を確認してサービスを提供するサービス提供システム、サービスの使用権の認証を行う認証装置及びサービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な媒体に関する。
【０００２】
【従来の技術】近年のネットワークの発達によってディジタル社会が到来し、欧米を中心とした電子商取引や電子マネーの運用が開始された今日、ＩＣ(Integrated Circuit)カードは、電子マネーを格納する電子財布などのさまざまなサービスを受けるための個人認証装置として重要な役割を担うようになっている。このような中でＩＣカードは、データを記憶するだけの単なるメモリーカードという位置づけから、ＣＰＵ(Central Processing Unit) を搭載しメモリに対するアクセス制限機能を有す

るようになり、さらに今日では高度な暗号演算機能を有し、ユーザ認証を行うものも登場している。

【０００３】ただし、ＩＳＯ(International Organization for Standardization)／ＩＥＣ(International Electrotechnical Commission) ７８１６準拠のＩＣカードには厚さの制限があるため、電源を内部に持つことができないという制約がある。また、製造コストの観点からも、ＩＣカード内に電源を持たせるのは有効ではない。このためＩＣカードの電源およびクロックは接続装置(Interface device)により供給され、電源の供給が断たれるとＩＣカード内部で時計機能を働かせておくことはできない。従って、ＩＣカードに時刻を書き込む必要があるときには、信頼できる端末でのみ時刻の更新ができるようにしていた。

【０００４】

【発明が解決しようとする課題】ところで、今後のＩＣカードを用いた認証を行うシステムの利用形態を考えると、利便性や通信コストの観点からローカルな環境やオフラインでの利用が必要とされる。このような環境において、例えば、ソフトウェアのライセンス管理をＩＣカードで行おうとすると、時間や期間によるアクセス管理を行う必要がある。その場合、時刻に関するデータをＩＣカードで管理しなければならない。

【０００５】しかし、ローカルな環境では、時間の管理をユーザの管理下にあるＰＣ(Personal Computer)により行わなければならず、ユーザの管理下にあるＰＣでは、いくらでもユーザによる時間の詐称が可能である。また、ＵＮＩＸ（登録商標）のクライアント・サーバシステムにおいては、時刻サーバを設けて、定期的にクライアントのマシンから時刻の同期を取る方法がある（下山智明他／ＳＵＮシステム管理／アスキー出版／ｐ．２４９（１９９１））が、このような管理は、クライアントとサーバが常に接続されていることが前提となり、またクライアントから同期要求を出すのでクライアントでの詐称は依然として容易であることに変わりはない。従って、ＩＣカードを用いた時間や期間によるライセンス管理が正常に機能し難いという問題点があった。

【０００６】なお、ネットワークを介したオンラインの利用制限が可能であれば、ＩＣカードの方で利用期間を管理する必要はなくなるが、今後のサービスの多様性を考慮すると、非現実的である。例えば、利用期限のあるサービスをユーザのローカルなコンピュータ等で実現するような場合、サービスを提供するソフトウェア等はオンラインで利用するよりもオフラインで利用した方がユーザには利便性があり、しかも経済的である。

【０００７】また、サービス提供者（プロバイダ）の方でも、ユーザの管理をサービスが利用される度に個別にオンラインで行うには、複雑な管理と非常に巨大なデータベースが必要となり、過大な設備投資が強いられる。従って、利便性や経済性を考慮すると、サービスの有効期間管理がオフラインで行えることが不可欠である。

【０００８】本発明はこのような問題に鑑みてなされたものであり、期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止できるサービス提供システムを提供することを目的とする。

【０００９】また、本発明の他の目的は、期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止できる認証装置を提供することである。

【００１０】さらに、本発明の別の目的は、期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止した認証処理をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することである。

【００１１】

【課題を解決するための手段】本発明では上記課題を解決するために、サービス提供装置と認証装置とから構成されるサービス提供システムであって、前記サービス提供装置は、特定のサービスに対応して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データを前記認証装置に出力する有効期限データ送出手段と、前記認証装置から返された使用許可応答に基づいて前記特定のサービスを提供するサービス提供手段と、を具備しており、前記認証装置は、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から受け取った前記有効期限データに含まれる前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を具備していることを特徴とするサービス提供システムが提供される。

【００１２】このサービス提供システムによれば、特定のサービスの提供を望むユーザは、サービス提供装置の有効期限データ送出手段を用いて、有効期限データを出力する。すると、認証用時刻が前記有効期限終了時刻より前の時刻である場合、認証装置内の認証手段により、サービス提供装置に対して使用許可応答が出力される。また、認証用時刻が有効期限データに含まれる有効期限開始時刻より前の時刻である場合、認証用時刻更新手段により、認証用時刻が有効期限開始時刻で示された時刻に更新される。一方、認証手段からの使用許可応答が出力されると、サービス提供手段による、ユーザへのサービスの提供が可能となる。

【００１３】また、本発明では上記課題を解決するために、サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻

とからなる有効期限データに基づいて該サービスの使用権の認証を行う認証装置であって、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を有することを特徴とする認証装置が提供される。

【００１４】この認証装置によれば、サービス提供装置から有効期限データが送られると、認証用時刻が前記有効期限終了時刻より前の時刻である場合、認証装置内の認証手段により、サービス提供装置に対して使用許可応答が出力される。また、認証用時刻が有効期限データに含まれる有効期限開始時刻より前の時刻である場合、認証用時刻更新手段により、認証用時刻が有効期限開始時刻で示された時刻に更新される。

【００１５】また、本発明では上記課題を解決するために、サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に変更する認証用時刻更新手段と、してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【００１６】この認証プログラムを記録した媒体に格納されたプログラムをコンピュータで実行すれば、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、および前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に変更する認証用時刻更新手段の各機能がコンピュータによって実現される。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は、本発明の原理構成図である。本発明のサービス提供システムは、ユーザに各種サービスを提供するサービス提供装置１０と、サービス提供装置１０の提供するサービスの使用権の有効性を認証する認証装置３０とで構成される。

【００１８】サービス提供装置１０において、有効期限データ送出手段１１は、特定のサービスに対応して設定された有効期限開始時刻２１と有効期限終了時刻２２とからなる有効期限データ２０を、認証装置３０へ出力する。サービス提供手段１２は、使用許可応答が入力された場合にのみ、特定のサービスの提供を可能とする。

【００１９】認証装置３０おいて、認証用時刻格納手段３１は、認証用時刻を保持する。認証手段３２は、サービス提供装置１０から有効期限データ２０を受け取ると、認証用時刻格納手段３１に格納されている認証用時刻と有効期限終了時刻２２とを比較し、認証用時刻が有効期限終了時刻２２より前の時刻である場合、サービス提供装置１０に対して使用許可応答を出力する。認証用時刻更新手段３３は、サービス提供装置１０から有効期限データ２０を受け取ると、認証用時刻格納手段３１に格納されている認証用時刻と有効期限開始時刻２１とを比較し、認証用時刻格納手段３１に格納されている認証用時刻が有効期限開始時刻２１より前の時刻である場合には、有効期限開始時刻２１を新たな認証用時刻として認証用時刻格納手段３１に格納する。

【００２０】このようなサービス提供システムによれば、サービスの提供者側は、各サービスに対応して有効期限データ２０を設定する。そして、特定のサービスの提供を受けようとするユーザは、サービス提供装置１０の有効期限データ送出手段１１により、特定のサービスに対応する有効期限データ２０を認証装置３０へ送出する。

【００２１】有効期限データ２０を受け取った認証装置３０では、認証手段３２により、認証用時刻格納手段３１内の認証用時刻と有効期限終了時刻とが比較され、認証用時刻が有効期限終了時刻より前の時刻である場合には、使用許可応答がサービス提供装置１０へ送られる。また、認証用時刻更新手段３３により、認証用時刻と有効期限開始時刻２１とが比較され、認証用時刻が有効期限開始時刻２１より前の時刻である場合には、有効期限開始時刻２１が新たな認証用時刻として認証用時刻格納手段３１に格納される。

【００２２】サービス提供装置１０のサービス提供手段１２は、使用許可応答を受け取った場合にのみ、ユーザに対してサービスを提供する。ここで、使用許可応答とは、サービス提供装置１０の入力データに対する認証装置３０の署名であったり、サービスを利用するために必要な情報であったりする。また、使用許可応答を送信する場合は、リプレイアタック等に対応するために、乱数を用いた秘密通信を用いてもよい。

【００２３】このようにして、サービス提供装置がオフ

ラインの状態でも、有効期限を指定したサービスの使用権の管理を行うことができる。しかも、認証用時刻は、サービスの提供を受ける際に有効期限開始時刻に更新され、その時刻を過去の時刻へ戻すことはできないため、ユーザが認証用時刻を詐称することはできない。

【００２４】本発明のサービス提供装置を用いて、ユーザはさまざまなサービスの提供を受けることができる。例えばそれは従来技術でも述べたように、ソフトウェアの使用権であったり、電子マネー等の有価情報であったり、さらには他のサービスを使用するためのチケットのようなものであったりする。

【００２５】次に、本発明の具体的な第１の実施の形態について、プロバイダが提供するソフトウェアのライセンス管理をＩＣカードで行う場合を例にとって説明する。図２は、ＩＣカードを用いた認証システムの概略構成を示す図である。ユーザが使用するパーソナルコンピュータ（ＰＣ）１１０は、インターネットなどのネットワーク１２０を介してセンタ１３０と繋がっている。センタ１３０では、ユーザの登録および、ユーザデータやユーザに提供したサービスの履歴等の管理が行われる。そして、センタ１３０は、ＰＣ１１０からの要求に応じて、カプセル化されたソフトウェア（以下、単に「カプセル」という）３００を提供する。ここでいうカプセル化とは、例えばＤＥＳ(Data Encryption Standard)等の暗号アルゴリズムを用いて暗号化し、そのままでは使用できないようにすることを指す。

【００２６】また、ＰＣ１１０には、ＲＳ－２３２Ｃ（アメリカ電子工業会によって規定されたデータ通信用インタフェース）などのインタフェースにより、リーダ／ライタ１４０が接続されている。ユーザは、このリーダ/ ライタ１４０にＩＣカード２００を接続することで、センタ１３０から取得したソフトウェアの使用権に関する認証を行うことができる。

【００２７】ＩＣカード２００は、ソフトウェアを提供するプロバイダ若しくはプロバイダの依頼を受けたセンタ１３０からユーザに渡されるものである。なお、この例では、ＰＣ１１０によってサービスを利用するものとしているが、サービスを利用するためのローカルな端末装置はＰＣには限定されず、例えばワークステーションであったり、サーバであったり、ＡＴＭ(Auto Teller Machine) 端末であったりする。

【００２８】図３は、カプセルの例を示す図である。カプセル３００は、ヘッダ部３１０と暗号化されたソフトウェア３２０とで構成される。ヘッダ部３１０はカプセルの起動を行うためのカプセル起動プログラム３１１と、ＩＣカードが認証ステップを行うために必要な認証データとに分けられる。

【００２９】カプセル起動プログラム３１１は、認証データ送出処理、ユーザ情報取得処理、ソフトウェア復号処理及びソフトウェア実行処理の各処理を、ＰＣ１１０に実行させるためのプログラムである。認証データ送出処理とは、カプセル３００内のヘッダ部３１０に含まれた認証データをＩＣカード２００へ送信する処理である。ユーザ情報取得処理とは、ユーザに対して、ユーザのＩＤ（ユーザ固有の識別情報）やパスワードの入力を促し、入力されたＩＤ等をＩＣカード２００に送信する処理である。ソフトウェア復号処理とは、ＩＣカード２００から復号鍵を受け取り、その復号鍵を用いて暗号化されたソフトウェア３２０を復号する処理である。ソフトウェア実行処理とは、復号されたソフトウェアを実行する処理である。

【００３０】また、ヘッダ部３１０内の認証データは、ソフトウェア認証データ３１２、ソフトウェア使用権認証データ３１３、有効期限認証データ３１４、及び暗号化された復号鍵３１５で構成される。ソフトウェア認証データ３１２には、例えば、ソフトウェアの識別子（ＩＤ）やプロバイダの署名が含まれる。ソフトウェア使用権認証データ３１３には、ユーザ認証が成功した際に、そのユーザに対応する使用権を認証するための情報が格納されている。有効期限認証データ３１４は、暗号化されたソフトウェア３２０の有効期限を示すデータである。暗号化された復号鍵３１５は、カプセル３００を復号するための復号鍵であり、この復号鍵を復号するための秘密情報（復号鍵）は、ＩＣカード２００内に予め格納されている。

【００３１】図４は、有効期限認証データ３１４の構造を示す図である。図のように、有効期限認証データ３１４には、有効期限開始時刻３１４ａ、有効期限終了時刻３１４ｂ及びセンタの署名３１４ｃが含まれている。ここでセンタの署名３１４ｃとは、例えば有効期限開始時刻３１４ａと有効期限終了時刻３１４ｂをセンタの署名鍵で署名したものである。このセンタの署名３１４ｃは、有効期限開始時刻３１４ａと有効期限終了時刻３１４ｂが詐称されていないことが確認できる機構が他に存在すれば必ずしも必要ではない。

【００３２】図５は、ＩＣカードのハードウェア構成を示す図である。ＩＣカード２００は、ＣＰＵ２１０を中心として、１つのコンピュータシステムが構築されている。ＣＰＵ２１０には、内部のシステムバスを介して他の各種要素が接続されている。ＲＡＭ(Random Access Memory)２２０は、ＣＰＵ２１０が処理すべきデータを一時的に格納する。ＲＯＭ(Read Only Memory)２３０は、ＩＣカード２００に必要な機能をＣＰＵ２１０に実行させるための認証プログラムが格納されている。入出力装置（Ｉ／Ｏ）２４０は、所定の規格に従って、リーダ／ライタ１４０との間でデータ通信を行う。ＰＲＯＭ(Programmable Read Only Memory) ２５０は、有効期限の認証に用いられるＩＣカード時刻や、暗号化された復号鍵３１５を復号するための秘密情報などが格納されている。

【００３３】このようなハードウェア構成のＩＣカード２００によって、以下のような処理機能が実現されている。図６は、ＩＣカードの処理機能を示すブロック図である。認証部２０１は、ＰＣ１１０から送られた認証データの内容に基づいて、カプセル３００の使用を認めるか否かの判断を行う。具体的には、使用を認める場合にはカプセル３００の使用を許可する旨の判定を行い、使用を認めない場合には、「エラー」の情報をＰＣ１１０に返す。認証部は、以下のような目的別の認証部を有している。

【００３４】ソフトウェア認証部２０１ａは、ソフトウェア認証データ３１２を参照し、カプセル３００が正当なプロバイダにより提供されたものかどうかを認証する。これによりコンピュータウイルス等の侵入を防ぐことができる。

【００３５】ユーザ認証部２０１ｂは、ＰＣ１１０から送られたユーザのＩＤやパスワードに基づいて、そのユーザがＩＣカード２００の所有者であることを認証する。ソフトウェア使用権認証部２０１ｃは、ソフトウェア使用権認証データ３１３に基づいて、このＩＣカード２００の所有者が、カプセル３００内のソフトウェアを使用する権利を有していることを認証する。例えば、カプセル３００内のソフトウェアがある一定以上の役職の者しか使用できない場合、このＩＣカード２００の所有者の役職を表す値が所定の値以下であれば、使用不可と判定する。

【００３６】有効期限認証部２０１ｄは、有効期限認証データ３１４の有効期限終了時刻３１４ｂとＩＣカード時刻２５１とを照らし合わせ、ＩＣカード時刻２５１が有効期限終了時刻３１４ｂ以前であることを認証する。

【００３７】以上の各認証部によりカプセル３００の使用が許可されると、その情報がＩＣカード時刻更新部２０２と復号鍵復号部２０３とに送られる。ＩＣカード時刻更新部２０２は、カプセル３００の使用が許可された際に、有効期限認証データ３１４の中の有効期限開始時刻３１４ａとＩＣカード時刻２５１とを比較する。そして、有効期限開始時刻の方が大きい場合には、ＩＣカード時刻２５１を有効期限開始時刻に書き換える。

【００３８】復号鍵復号部２０３は、ＰＲＯＭ２５０に格納されている秘密情報２５２を用いて、暗号化された復号鍵３１５を復号する。そして、復号された復号鍵を、ＰＣ１１０に転送する。

【００３９】以上のような構成のシステムにおいて、まず、プロバイダにより作成されたソフトウェアは、センタ１３０またはそれに準ずる機関によりカプセル化され、カプセル３００が生成される。

【００４０】次に、ユーザはネットワーク１２０またはＣＤＲＯＭ等によりカプセル３００を入手する。そして、ユーザは、自己の所持するＩＣカード２００をリーダ／ライタ１４０に接続し、入手したカプセル３００をＰＣ１１０で起動する。

【００４１】ＰＣ１１０は、カプセル３００の起動命令を受けると、カプセル起動プログラム３１１を読み込み、その命令にしたがってＩＣカード２００と通信し、ＩＣカード２００に認証データを渡す。すると、ＩＣカード２００が認証ステップを実行することで認証が行われる。正しく認証されればソフトウェアを復号するための復号鍵がＩＣカード２００からＰＣ１１０に送られる。ＰＣ１１０は、受け取った復号鍵で暗号化されたソフトウェア３２０を復号し、平文となったソフトウェアを実行する。

【００４２】なお、カプセル起動プログラム３１１とＩＣカード２００と間の通信はＩＣカードのセキュアメッセージング機能を用いることで復号鍵等が露呈することを防ぐことが出来る。また、ソフトウェアが復号された後もカプセル起動プログラムを経由しなければ実行できないようにすることで、ソフトウェアの使用管理を確実にすることが出来る。

【００４３】以下に、認証手順の詳細を説明する。図７は、第１の実施の形態の認証手順を示すフローチャートである。図中の破線から左側がカプセル起動プログラム３１１に基づくＰＣ１１０の処理を表し、破線から右側がＩＣカード２００の処理を表す。

【００４４】［Ｓ１］まずカプセル起動プログラム３１１を起動したＰＣ１１０は、カプセル３００の認証データをＩＣカード２００に送信する。なお、ここにいう認証データには、ユーザＩＤとパスワードも含まれるものとする。

【００４５】ＩＣカード２００では認証データ等を用いて、以下の認証処理が行われる。

［Ｓ２］ソフトウェア認証部２０１ａは、まずソフトウェア認証データ３１２に基づいてソフトウェアの認証を行う。ソフトウェアが正しいと判断されればステップＳ３に進み、ソフトウェアが正しくないと判断されればステップＳ６に進む。

【００４６】［Ｓ３］ユーザ認証部２０１ｂは、ユーザがＰＣ１１０に入力したユーザＩＤとパスワードに基づいてユーザの認証を行う。ユーザが正しいと判断されればステップＳ４に進み、ユーザが正しくないと判断されればステップＳ６に進む。

【００４７】［Ｓ４］ソフトウェア使用権認証部２０１ｃは、ソフトウェア使用権認証データ３１３に基づいてソフトウェア使用権の認証を行う。ソフトウェアの使用権があると判断された場合にはステップＳ５に進み、ソフトウェアの使用権がないと判断された場合にはステップＳ６に進む。

【００４８】なお、上記ステップＳ２～Ｓ４までの認証方法に関しては本発明では特に規定せず、それらは例えばＲＳＡ(Rivest Shamir Adleman) 暗号を用いた認証方法であったりＤＥＳ－ＭＡＣ(Message Authentication

Cord) を用いたものであったりする。

【００４９】［Ｓ５］有効期限認証部２０１ｄは、有効期限認証データ３１４に含まれるセンタの署名３１４ｃに基づいて、有効期限開始時刻３１４ａと有効期限終了時刻３１４ｂが正しいことを検証する。そして、ＩＣカード２００のＰＲＯＭ２５０に記憶されているＩＣカード時刻２５１が有効期限終了時刻３１４ｂ以下であるかどうかを確認する。有効期限認証データ３１４が正しいことの検証と、ＩＣカード時刻２５１が有効期限終了時刻以下であることの検証の結果が正しければステップＳ７に進み、それらの検証の結果が正しくなければステップＳ６に進む。

【００５０】［Ｓ６］認証部２０１は、ステップＳ２～Ｓ５の認証に失敗した場合は、ＰＣ１１０に対してエラーを返し、処理を終了する。

［Ｓ７］ＩＣカード時刻更新部２０２は、ＩＣカード時刻２５１が有効期限開始時刻３１４ａより小さいか否かを判断し、ＩＣカード時刻２５１の方が小さい場合には、ＩＣカード時刻２５１を有効期限開始時刻３１４ａで示された時刻に書き換える。

【００５１】［Ｓ８］復号鍵復号部２０３は、暗号化された復号鍵３１５を、ＰＲＯＭ２５０に保持されている秘密情報２５２を用いて復号し、ＰＣ１１０に返信する。

［Ｓ９］復号鍵を受け取ったＰＣ１１０は、カプセル起動プログラム３１１の指令に基づき、暗号化されたソフトウェア３２０を復号し、そのソフトウェアを実行する。この時、ソフトウェア３２０は完全に復号されるわけではなく、実行する部分のみが復号されて揮発性メモリに展開されるようにしておき、ソフトウェアが終了されると復号され揮発性メモリに展開されたソフトウェアは消去するようにしておけば、復号されたソフトウェアが不正に使用されることはない。

【００５２】このように、カプセルの有効期限を有効期限開始時刻３１４ａと有効期限終了時刻３４１ｂとで管理し、カプセルの実行時にＩＣカード時刻２５１と比較しＩＣカード時刻２５１が有効期限開始時刻３１４ａより小さい場合はＩＣカード時刻２５１を有効期限開始時刻３１４ａで更新するようにしたことにより、ユーザが新しいカプセルをセンタまたはプロバイダから入手し実行するとＩＣカード時刻が更新され、新しいカプセルの有効期限開始時刻よりも小さい有効期限終了時刻が設定されているカプセルは使用することができなくなる。その結果、ＩＣカードに時計を持たせなくてもソフトウェア使用権の有効期限管理を行うことが可能である。

【００５３】例えば、１９９７年７月１から１ヶ月間の有効期限（有効期限開始時刻：１９９７年７月１日、有効期限終了時刻：１９９７年７月３１日）が設定されたカプセルを実行すると、ＩＣカード時刻には、必ず１９９７年７月１以降の時刻が設定される。すると、その後は、有効期限終了時刻が１９９７年６月３０日以前であるカプセルを実行することは出来ない。

【００５４】以下に、本発明に関連する技術を、他の実施の形態として説明する。なお、図２～図５に示した構成は後述する他の実施の形態においても同様であるため、各実施の形態の説明においても図２～図５に示した符号を用いて説明する。ただし、ＩＣカードの処理機能に関しては、個別の符号を付して説明するものとする。

【００５５】まず、第２の実施の形態について説明する。この実施の形態は、ＩＣカードの時刻の更新をＰＣからの時刻設定コマンドによって行うものである。図８は、第２の実施の形態におけるＩＣカードの処理機能を示すブロック図である。本実施の形態のＩＣカード４００の処理機能の中で、認証部４０１中のソフトウェア認証部４０１ａ、ユーザ認証部４０１ｂ及びソフトウェア使用権認証部４０１ｃと、復号鍵復号部４０３との有する機能は、図６に示した第１の実施の形態における同名の構成要素と同じであるため、説明を省略する。すなわち、本実施の形態は、有効期限認証部４０１ｄとＩＣカード時刻更新部４０２との処理機能が、第１の実施の形態と異なる。また、第１の実施の形態と同様に、ＩＣカード４００内には、ＩＣカード時刻４５１と秘密情報４５２とが保持されている。

【００５６】ＰＣ１１０は、ユーザからの入力に応じて、若しくは所定のタイミングで時刻設定処理を行う。時刻設定処理では、ＰＣ１１０内部の時計時刻を時刻設定コマンドに含めて、ＩＣカード４００に送る。

【００５７】ＩＣカード時刻更新部４０２は、ＰＣ１１０から時刻設定コマンドを受け取ると、ＩＣカード時刻４５１の更新を行い、更新ステータス（「正常終了」又は「エラー」）をＰＣ１１０に返す。

【００５８】図９は、時刻設定コマンドが発行された際の処理手順を示すフローチャートである。この図において破線から左側をＰＣ１１０、破線から右側をＩＣカード４００とする。

【００５９】［Ｓ１１］ＰＣ１１０によって発行された時刻設定コマンドにより、ＰＣ時刻（ＰＣ１１０内の時計の時刻）がＩＣカード４００のＩＣカード時刻更新部４０２に渡される。

【００６０】［Ｓ１２］ＰＣ時刻を受け取ったＩＣカード時刻更新部４０２は、ＰＣ時刻とＩＣカード時刻４５１とを比較し、「ＰＣ時刻＞ＩＣカード時刻」であった場合はステップＳ１４に進み、「ＰＣ時刻＞ＩＣカード時刻」が成り立たなかった場合はステップＳ１３に進む。

【００６１】［Ｓ１３］ＩＣカード時刻更新部４０２は、「ＰＣ時刻＞ＩＣカード時刻」が成り立たなかった場合、すなわち現在のＩＣカード時刻４５１よりも小さな値で時刻を更新しようとした場合は、ＰＣ１１０にエラーステータスを返し、処理を終了する。

【００６２】［Ｓ１４］ＩＣカード時刻更新部４０２は、「ＰＣ時刻＞ＩＣカード時刻」であった場合、ＩＣカード時刻４５１をＰＣ時刻で更新し、ＰＣ１１０に正常終了のステータスを返す。

【００６３】このように時刻設定コマンドでは、ＩＣカードの時刻を進める方には更新できるが、時刻を戻す方には更新できないようになっている。図１０は、第２の実施の形態の認証手順を示すフローチャートである。この図において破線から左側がカプセル起動プログラムに基づいて処理を実行するＰＣ１１０を表し、破線から右側がＩＣカード４００を表す。

【００６４】［Ｓ２１］ＰＣ１１０においてカプセル起動プログラム３１１が起動されると、カプセルの認証データがＩＣカード４００へ送信される。ＩＣカード４００では認証データ等を用いて、以下の認証処理が行われる。

【００６５】［Ｓ２２］ソフトウェア認証部４０１ａは、ソフトウェア認証データ３１２に基づいてソフトウェアの認証を行う。ソフトウェアが正しいと判断されればステップＳ２３に進み、ソフトウェアが正しくないと判断されればステップＳ２６に進む。

【００６６】［Ｓ２３］ユーザ認証部４０１ｂは、ユーザがＰＣ１１０に入力したユーザＩＤとパスワードに基づいてユーザの認証を行う。ユーザが正しいと判断されればステップＳ２４に進み、ユーザが正しくないと判断されればステップＳ２６に進む。

【００６７】［Ｓ２４］ソフトウェア使用権認証部４０１ｃは、ソフトウェア使用権認証データ３１３に基づいてソフトウェア使用権の認証を行う。ソフトウェアの使用権があると判断された場合にはステップＳ２５に進み、ソフトウェアの使用権がないと判断された場合にはステップＳ２６に進む。

【００６８】［Ｓ２５］有効期限認証部４０１ｄは、有効期限認証データ３１４に含まれるセンタの署名３１４ｃに基づいて、有効期限開始時刻３１４ａと有効期限終了時刻３１４ｂが正しいことを検証する。そして、ＩＣカード４００に記憶されているＩＣカード時刻４５１が有効期限開始時刻３１４ａ以上であり、かつ有効期限終了時刻３１４ｂ以下であるかどうかを確認する。有効期限認証データが正しいことの検証と、ＩＣカード時刻４５１が有効期限内であることの検証の結果が正しければステップＳ２７に進み、それらの検証の結果が正しくなければステップＳ２６に進む。

【００６９】［Ｓ２６］認証部４０１は、ステップＳ２２～Ｓ２５のいずれかの認証に失敗した場合はＰＣ１１０に対してエラーを返し、処理を終了する。

［Ｓ２７］復号鍵復号部４０３は、暗号化された復号鍵３１５を、秘密情報４５２を用いて復号し、ＰＣ１１０に返信する。

【００７０】［Ｓ２８］復号鍵を受け取ったＰＣ１１０は、カプセル起動プログラム３１１の指令に基づき、その復号鍵を用い暗号化されたソフトウェア３２０を復号し、そのソフトウェアを実行する。

【００７１】以上のような処理機能を有するＰＣ１１０とＩＣカード４００を用い、ユーザが、まず第１のカプセルを実行し、次に第２のカプセルを実行する場合を想定し、本実施の形態の処理手順を具体的に説明する。

【００７２】図１１は、カプセルの有効期限とＩＣカード時刻の変化とを示す図である。第１のカプセルの有効期限４１は、１９９７年７月１日から１９９７年７月３１日までであり、第２のカプセルの有効期限４２は、１９９７年９月１日から１９９７年９月３０日までである。なお、現在の正しい時刻は「１９９７年９月１５日」であるが、ユーザは、ＰＣの時刻をごまかしてソフトウェアを利用しているものとする。また、カプセルを実行前のＩＣカード時刻には、１９９７年７月１日以前の時刻５１が設定されているものとする。

【００７３】ここで、ユーザが第１のカプセルを実行する場合には、時刻５１に設定されているＩＣカード時刻４５１を、第１のカプセルの有効期限４１内の時刻に更新しなければならない。そこでユーザは、ＰＣ時刻を「１９９７年７月１５日」に設定する。そして、ＰＣ１１０から時刻設定コマンドが発行されると、その時刻５２がＩＣカード時刻４５１として設定される。これにより、ユーザは不正に第１のカプセルを実行できる。

【００７４】次に、ユーザが新しい第２のカプセルを入手して実行する場合には、時刻５２に設定されているＩＣカード時刻４５１を、第２のカプセルの有効期限４２内の時刻に更新しなければならない。そこでユーザは、ＰＣ時刻を正しい時刻「１９９７年９月１５日」に設定し、ＰＣ１１０から時刻設定コマンドを発行する。すると、その時刻５３がＩＣカード時刻４５１になる。これにより、ユーザは第２のカプセルを正当に実行できる。

【００７５】その後、ユーザが第１のカプセルを実行しようとしてもＩＣカード時刻４５１には、時刻５３が設定されており第１のカプセルの有効期限４１の範囲外となっているので、再び第１のカプセルを使用することは出来なくなる。また、ＩＣカード時刻４５１は、時刻を増加させることのみが可能であるため、ＩＣカード時刻４５１を第１のカプセルの有効期限４１の範囲内に戻すことは出来ない。

【００７６】このようにカプセルの有効期限を有効期限開始時刻と有効期限終了時刻とで管理し、カプセルの実行時にＩＣカード時刻と比較しＩＣカード時刻が有効期限内でないと実行できないようにしてあるので、ユーザが新しいカプセルをセンタまたはプロバイダから入手し実行しようとするとＩＣカード時刻を更新しなければならない。そのため、新しいカプセルの有効期限開始時刻よりも小さい有効期限終了時刻が設定されているカプセルは使用することができなくなり、ＩＣカードに時計を

持たせなくてもソフトウェア使用権の有効期限管理を行うことが可能である。

【００７７】次に、第３の実施の形態について説明する。この実施の形態は、使用期限の管理に加えて利用回数の管理を行うことにより、より確実に不正使用の防止を図ったものである。

【００７８】図１２は、第３の実施の形態におけるＩＣカードの処理機能を示すブロック図である。本実施の形態のＩＣカード５００の処理機能の中で、ソフトウェア認証部５０１ａ、ユーザ認証部５０１ｂ、ソフトウェア使用権認証部５０１ｃ、有効期限認証部５０１ｄ及び復号鍵復号部５０３の有する機能は、図８に示した第２の実施の形態における同名の構成要素と同じであるため、説明を省略する。

【００７９】利用回数カウンタ５０４は、ＩＣカード５００がユーザに渡される際に、プロバイダ若しくはセンタ１３０によって所定の値が初期値として設定されており、認証部５０１により使用が許可される度に、設定されている値を１だけ減算する。

【００８０】認証部５０１内に設けられた利用回数制限認証部５０１ｅは、利用回数カウンタ５０４の値が０であればソフトウェアの使用を許否し、０以外の値であればソフトウェアの使用を認める。

【００８１】乱数生成部５０５は、ＰＣ１１０からチャレンジ要求を受け取ると、乱数を生成する。乱数暗号化部５０６は、乱数生成部５０５が生成し乱数を秘密鍵を用いて暗号化し、チャレンジとしてＰＣ１１０へ転送する。

【００８２】レスポンス検証部５０７は、ＰＣ１１０からのレスポンスをセンタの公開鍵で復号し、レスポンスに含まれる乱数と乱数生成部５０５で生成した乱数とが一致するか否かに基づき、レスポンスが正しいことを検証する。レスポンスが正しくない場合には、ＰＣ１１０にエラーを返す。レスポンスが正しければ、その旨の情報を、ＩＣカード時刻更新部５０２とカウンタ初期化部５０８とに伝える。その際、センタ時刻の情報をＩＣカード時刻更新部５０２へ渡す。

【００８３】ＩＣカード時刻更新部５０２は、レスポンス検証部５０７からレスポンスが正しい旨の情報を受け取ると、センタ時刻がＩＣカード時刻より大きい場合には、レスポンス検証部５０７から送られたセンタ時刻で、ＩＣカード時刻５５１を更新する。

【００８４】カウンタ初期化部５０８は、レスポンス検証部５０７からレスポンスが正しい旨の情報を受け取ると、利用回数カウンタ５０４を初期化する。このような機能を有するＩＣカード５００を用い、以下のような認証処理を行う。

【００８５】図１３は、第３の実施の形態の認証手順を示すフローチャートである。この図において破線から左側がカプセル起動プログラムに基づいて処理を実行するＰＣ１１０を表し、破線から右側がＩＣカード５００を表す。

【００８６】［Ｓ３１］ＰＣ１１０においてカプセル起動プログラム３１１が起動されると、カプセルの認証データがＩＣカード５００へ送信される。ＩＣカード５００では認証データ等を用いて、以下の認証処理が行われる。

【００８７】［Ｓ３２］ソフトウェア認証部５０１ａは、ソフトウェア認証データ３１２に基づいてソフトウェアの認証を行う。ソフトウェアが正しいと判断されればステップＳ３３に進み、ソフトウェアが正しくないと判断されればステップＳ３７に進む。

【００８８】［Ｓ３３］ユーザ認証部５０１ｂは、ユーザがＰＣ１１０に入力したユーザＩＤとパスワードに基づいてユーザの認証を行う。ユーザが正しいと判断されればステップＳ３４に進み、ユーザが正しくないと判断されればステップＳ３７に進む。

【００８９】［Ｓ３４］ソフトウェア使用権認証部５０１ｃは、ソフトウェア使用権認証データ３１３に基づいてソフトウェア使用権の認証を行う。ソフトウェアの使用権があると判断された場合にはステップＳ３５に進み、ソフトウェアの使用権がないと判断された場合にはステップＳ３７に進む。

【００９０】［Ｓ３５］有効期限認証部５０１ｄは、有効期限認証データ３１４に含まれるセンタの署名３１４ｃに基づいて、有効期限開始時刻３１４ａと有効期限終了時刻３１４ｂが正しいことを検証する。そして、ＩＣカード５００に記憶されているＩＣカード時刻５５１が有効期限開始時刻３１４ａ以上であり、かつ有効期限終了時刻３１４ｂ以下であるかどうかを確認する。有効期限認証データが正しいことの検証と、ＩＣカード時刻５５１が有効期限内であることの検証の結果が正しければステップＳ３６に進み、それらの検証の結果が正しくなければステップＳ３７に進む。

【００９１】［Ｓ３６］利用回数制限認証部５０１ａは、利用回数カウンタが０でないことを確かめ、利用回数カウンタが０であればステップＳ３７に進み、利用回数カウンタが０でない場合にはステップＳ３８に進む。

【００９２】［Ｓ３７］認証部５０１は、ステップＳ３２～Ｓ３６のいずれかの認証に失敗した場合はＰＣ１１０に対してエラーを返し、処理を終了する。

［Ｓ３８］利用回数カウンタ５０４は、認証部５０１から使用を許可する旨の信号が出力されると、設定されている値を１だけ減算する。

【００９３】［Ｓ３９］暗号化された復号鍵をＩＣカード５００の秘密情報５５２を用いて復号しＰＣ１１０に返信する。

［Ｓ４０］ＰＣ１１０は、カプセル起動プログラム３１１の命令に従い、返信された復号鍵を用い暗号化されたソフトウェア３２０を復号しソフトウェアを実行する。

【００９４】なお、以上の説明では利用回数カウンタ５０４がある値から減算され０になるとカプセルを実行できないようにしているが、逆に利用回数カウンタを０からスタートさせ、ある値になるとカプセルを実行できないようにしてもよい。

【００９５】上記の説明で利用回数カウンタが０となりカプセルを実行できなくなったＩＣカードは、以下に示す操作により再びカプセルを実行できるようにすることが出来る。

【００９６】図１４は、利用回数カウンタのリセット処理の手順を示すフローチャートである。この図において、破線から左側はＰＣ１１０、破線から右側はＩＣカード５００を表す。

【００９７】［Ｓ４１］ＰＣ１１０は、ＩＣカード５００へチャレンジ要求を出す。

［Ｓ４２］ＩＣカード５００がチャレンジ要求を受け取ると、乱数生成部５０５が乱数ｒを生成する。

【００９８】［Ｓ４３］乱数暗号化部５０６が、乱数ｒを公開鍵暗号方式に対応したＩＣカード５００の秘密鍵で暗号化し、それをチャレンジとしてＰＣ１１０に返信する。　［Ｓ４４］ＰＣ１１０はＩＣカード５００からチャレンジを受け取ると、そのチャレンジをセンタ１３０に送信し、センタ１３０からレスポンスを得る。レスポンスの構造としては、例えばＩＣカードから受け取った乱数とセンタ時刻とを連結し公開鍵暗号方式に対応したセンタ１３０の秘密鍵で署名した構造となっている。

【００９９】［Ｓ４５］ＰＣ１１０は、センタ１３０から受け取ったレスポンスをＩＣカード５００へ送信する。

［Ｓ４６］レスポンス検証部５０７はレスポンスの検証を行う。レスポンス検証の手順としてはあらかじめＩＣカード５００に登録されている公開鍵暗号方式に対応したセンタ１３０の公開鍵で署名の検証をし、乱数生成部５０５が生成した乱数ｒとレスポンス中のｒが一致することを確認する。レスポンスの検証に成功した場合にはステップＳ４８に進み、検証に失敗した場合にはステップＳ４７へ進む。

【０１００】［Ｓ４７］レスポンスの検証に失敗した場合には、レスポンス検証部５０７がＰＣ１１０に対してエラーを返し、処理を終了する。

［Ｓ４８］センタ時刻がＩＣカード時刻より大きい場合は、ＩＣカード時刻更新部５０２が、レスポンスに含まれるセンタ時刻をＩＣカード時刻５５１に代入する。

【０１０１】［Ｓ４９］また、カウンタ初期化部５０８が、利用回数カウンタ５０４を初期値に戻し再びカプセルが使用できるようにする。

［Ｓ５０］レスポンス検証部５０７がＰＣ１１０に対して、正常終了のステータスを返す。

【０１０２】このようにカプセルの使用を回数で制限し、利用回数制限に達したらカプセルを利用できなくし、その後センタと交信しセンタの時刻でＩＣカード時刻を更新した場合にのみ、再びカプセルを使用可能とすることで、ＩＣカードの時刻を管理することが可能になる。

【０１０３】なお、上記の説明で乱数を暗号化する際や、レスポンスを検証する際に公開鍵暗号方式を例にとって説明したが、これは本発明を何ら限定するものではなくＩＣカード５００とセンタ１３０とにおけるデータ交換の正当性を保証できるものであれば代用可能である。また、乱数ｒを検証データとして用いたが、これは必ずしも乱数である必要はなくチャレンジ要求に対して毎回値が更新されるものであればよい。

【０１０４】また、レスポンスに利用回数の更新値を持たせることで、利用回数カウンタを任意の値だけ更新できるようにすることも可能である。次に、第４の実施の形態について説明する。この実施の形態は、センタからのＩＣカードへのデータにセンタ時刻を含め、そのセンタ時刻によりＩＣカード時刻を更新するものである。

【０１０５】図１５は、第４の実施の形態におけるＩＣカードの処理機能を示すブロック図である。本実施の形態のＩＣカード６００の処理機能の中で、認証部６０１（ソフトウェア認証部６０１ａ、ユーザ認証部６０１ｂ、ソフトウェア使用権認証部６０１ｃ及び有効期限認証部６０１ｄを含む）と復号鍵復号部６０３との有する機能は、図６に示した第１の実施の形態における同名の構成要素と同じであるため、説明を省略する。また、第１の実施の形態と同様に、ＩＣカード６００内には、ＩＣカード時刻６５１と秘密情報６５２とが保持されている。

【０１０６】センタ署名検証部６０４は、センタからのデータをＰＣ１１０を介して受け取ると、そのセンタの署名を検証する。正しければ、その旨をＩＣカード時刻更新部６０２に通知する。また、センタの署名が正しくなければ「エラー」の更新ステータスをＰＣ１１０に返す。

【０１０７】ＩＣカード時刻更新部６０２は、ＩＣカード時刻６５１とセンタ時刻とを比較し、センタ時刻の方が大きければ、ＩＣカード時刻６５１をセンタ時刻に更新する。

【０１０８】図１６は、センタからのデータの例を示す図である。センタからのデータ６０は、ＩＣカード６００に発行するデータ６１、センタからのデータ６０が発行されたときのセンタ時刻６２、およびデータ６１とセンタ時刻６２に対するセンタの署名６３で構成される。ここでセンタからのデータとは、センタから発行された任意のデータを指し、例えばカプセルそのものであったり、何かのサービスを取得するためのチケットのようなものであったり、ただ単にセンタからのメッセージだったりする。

【０１０９】図１７は、第４の実施の形態におけるＩＣカード時刻の更新手順を示すフローチャートである。この図において破線から左側がＰＣ１１０を表し、破線から右側がＩＣカード６００を表す。

【０１１０】［Ｓ６１］ＰＣ１１０はＩＣカード６００にセンタ１３０からのデータ６０を送信する。

［Ｓ６２］センタ署名検証部６０４は、センタ１３０からのデータ６０を受け取ると、センタの署名の検証を行いＩＣカード６００に発行するデータ６１とセンタ時刻６２が正当であることを検証する。検証に成功した場合は、データ６０に応じた処理を行った後、ステップＳ６４へ進む。検証に失敗した場合は、ステップＳ６３に進む。

【０１１１】［Ｓ６３］センタ署名検証部６０４は、ＰＣ１１０に対してエラーを返し、処理を終了する。

［Ｓ６４］ＩＣカード時刻更新部６０２は、センタ時刻６２とＩＣカード時刻６５１とを比較する。センタ時刻６２がＩＣカード時刻６５１より大きい場合にはステップＳ６５に進み、それ以外の場合にはステップＳ６６に進む。

【０１１２】［Ｓ６５］ＩＣカード時刻更新部６０２は、センタ時刻６２をＩＣカード時刻６５１に代入する。

［Ｓ６６］ＩＣカード時刻更新部６０２は、ＰＣ１１０に対し、正常終了の更新ステータスを返す。

【０１１３】このようにセンタからＩＣカードに発行されるデータにはセンタ時刻とセンタの署名をつけるようにすることで、ＩＣカードの時刻管理を可能とすることが出来る。

【０１１４】なお、上記のＩＣカードの有する機能の処理内容は、ＲＯＭに格納された認証プログラムをＩＣカード内のＣＰＵが実行することで実現されているが、この認証プログラムを他の記録媒体に格納しておくこともできる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場を流通させる場合には、ＣＤ－ＲＯＭやフロッピー（登録商標）ディスケット等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【０１１５】

【発明の効果】以上説明したように本発明のサービス提供システムでは、サービスの有効期限を有効期限開始時刻と有効期限終了時刻とで管理し、認証装置の認証用時刻を有効期限開始時刻を用いて更新するようにしたため、ローカルなサービス提供装置であっても、内部に時計を持たない認証装置を用いてサービスの利用権の有効期限の管理を行うことが可能となる。

【０１１６】また、本発明の認証装置では、サービス提供装置からの要求に応じて有効期限の認証を行うと共に、認証用時刻を有効期限開始時刻を用いて更新するようにしたため、内部に時計を持たずに、有効期限の認証を行うことが可能となる。

【０１１７】また、本発明の認証プログラムを記録したコンピュータ読み取り可能な記録媒体では、サービス提供装置からの要求に応じて有効期限の認証を行うと共に、認証用時刻を有効期限開始時刻を用いて更新するようなプログラムを格納したため、格納したプログラムをコンピュータで実行させれば、内部時計を用いない有効期限の認証をコンピュータに行わせることが可能となる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】ＩＣカードを用いた認証システムの概略構成を示す図である。

【図３】カプセルの例を示す図である。

【図４】有効期限認証データの構造を示す図である。

【図５】ＩＣカードのハードウェア構成を示す図である。

【図６】ＩＣカードの処理機能を示すブロック図である。

【図７】第１の実施の形態の認証手順を示すフローチャートである。

【図８】第２の実施の形態におけるＩＣカードの処理機能を示すブロック図である。

【図９】時刻設定コマンドが発行された際の処理手順を示すフローチャートである。

【図１０】第２の実施の形態の認証手順を示すフローチャートである。

【図１１】カプセルの有効期限とＩＣカード時刻の変化とを示す図である。

【図１２】第３の実施の形態におけるＩＣカードの処理機能を示すブロック図である。

【図１３】第３の実施の形態の認証手順を示すフローチャートである。

【図１４】利用回数カウンタのリセット処理の手順を示すフローチャートである。

【図１５】第４の実施の形態におけるＩＣカードの処理機能を示すブロック図である。

【図１６】センタからのデータの例を示す図である。

【図１７】第４の実施の形態におけるＩＣカード時刻の更新手順を示すフローチャートである。

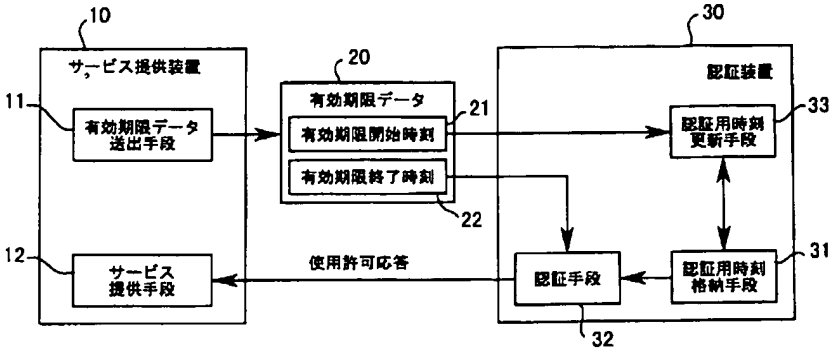
【符号の説明】

１０　サービス提供装置
１１　有効期限データ送出手段
１２　サービス提供手段
２０　有効期限データ

23　　24

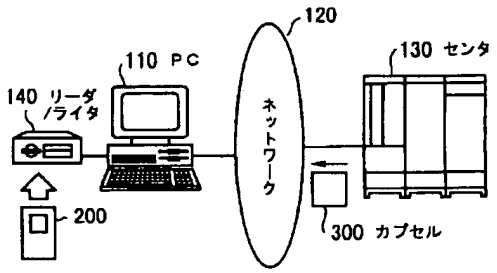
２１　有効期限開始時刻
２２　有効期限終了時刻
３０　認証装置
３１　認証用時刻格納手段
３２　認証手段
３３　認証用時刻更新手段

【図１】

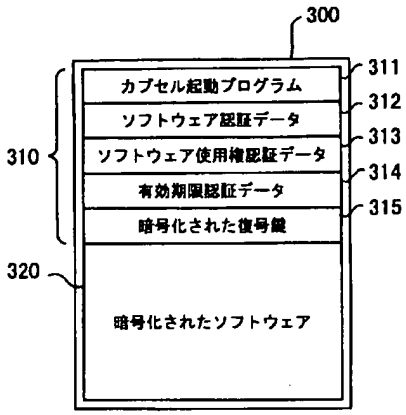


【図２】

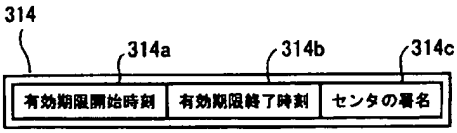
【図３】

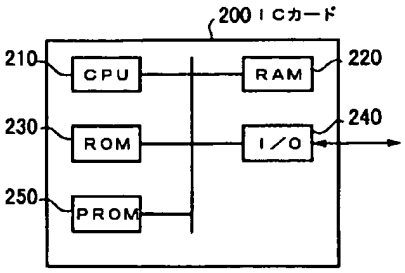


【図４】



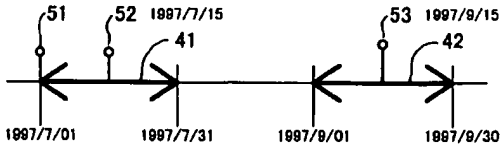
【図５】

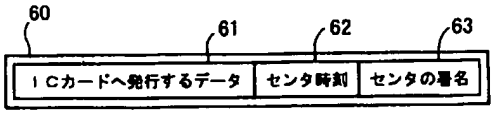




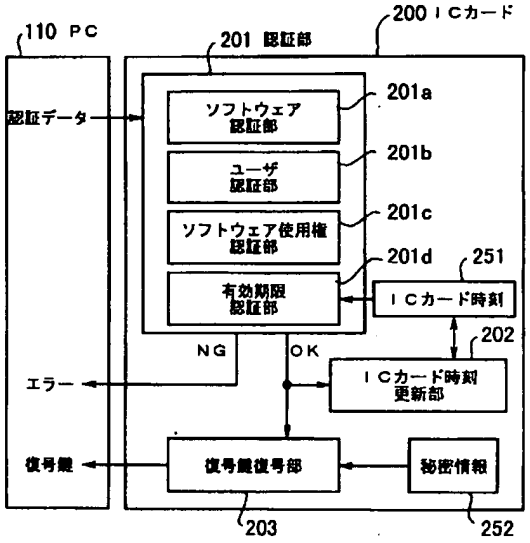
【図１１】

【図１６】

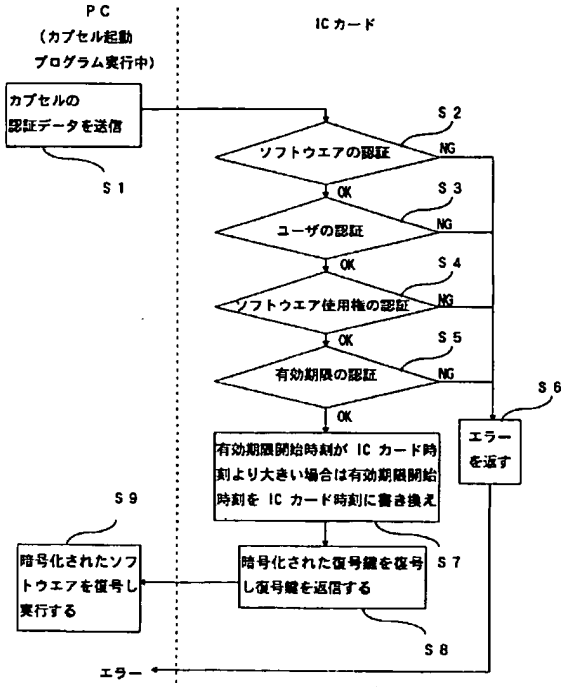




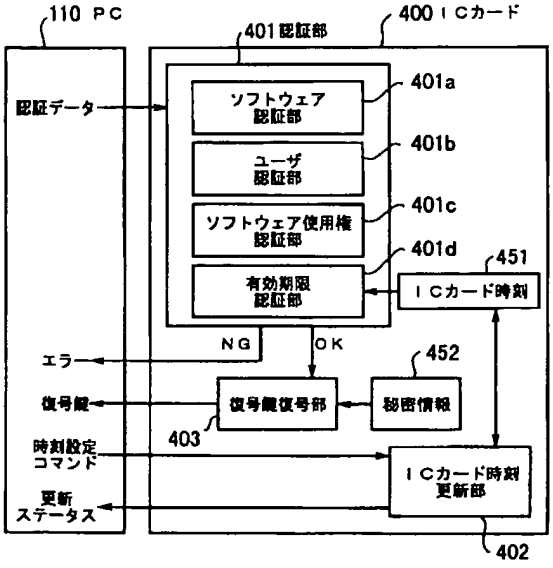
【図６】


110 PC
200 ＩＣカード
201 認証部
認証データ
ソフトウェア認証部
201a
ユーザ認証部
201b
ソフトウェア使用権認証部
201c
有効期限認証部
201d
251
ＩＣカード時刻
202
NG
OK
エラー
ＩＣカード時刻更新部
復号鍵
復号鍵復号部
秘密情報
203
252

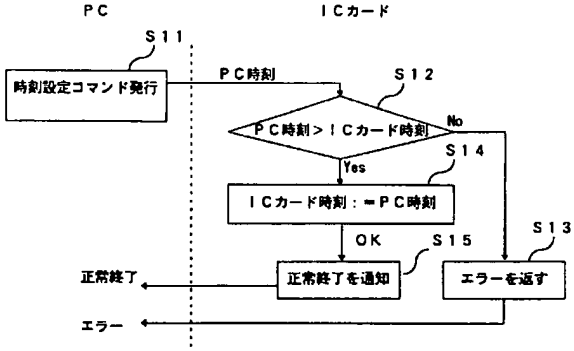
【図７】


PC
（カプセル起動プログラム実行中）
ICカード
カプセルの認証データを送信
S1
ソフトウエアの認証
S2
NG
OK
ユーザの認証
S3
ソフトウエア使用権の認証
S4
有効期限の認証
S5
エラーを返す
S6
有効期限開始時刻がICカード時刻より大きい場合は有効期限開始時刻をICカード時刻に書き換え
S7
暗号化された復号鍵を復号し復号鍵を返信する
S8
暗号化されたソフトウエアを復号し実行する
S9
エラー

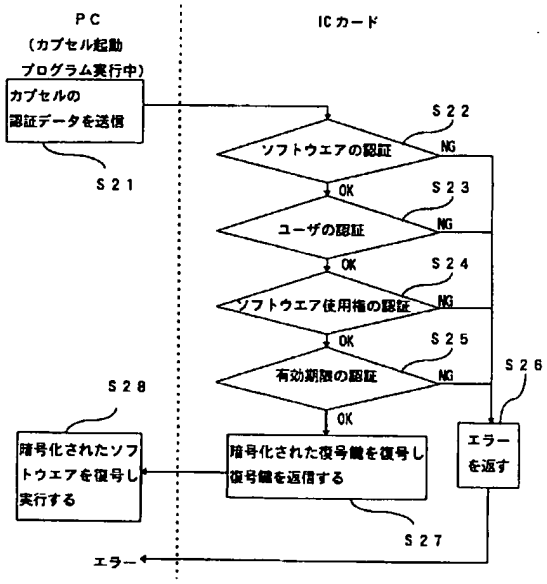
【図８】


110 PC
400 ＩＣカード
401 認証部
認証データ
ソフトウェア認証部
401a
ユーザ認証部
401b
ソフトウェア使用権認証部
401c
有効期限認証部
401d
451
ＩＣカード時刻
NG
OK
エラー
452
復号鍵
復号鍵復号部
秘密情報
403
時刻設定コマンド
ＩＣカード時刻更新部
更新ステータス
402

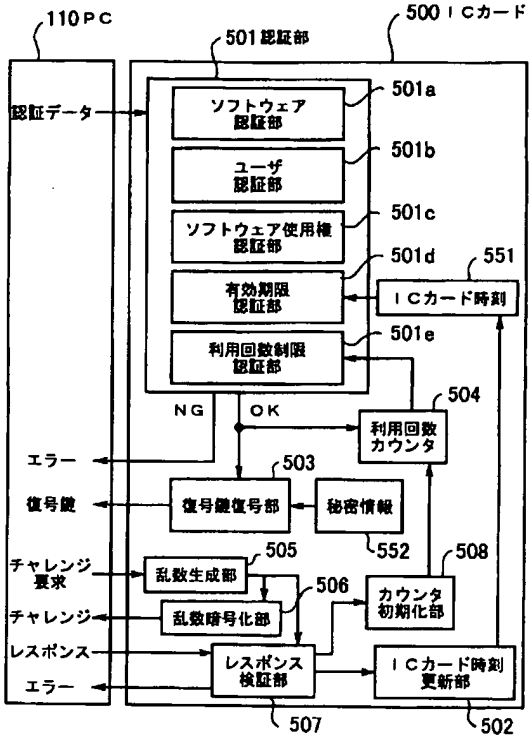
【図９】


PC
ＩＣカード
S11
時刻設定コマンド発行
PC時刻
S12
PC時刻＞ＩＣカード時刻
No
Yes
S14
ＩＣカード時刻：＝PC時刻
OK
S15
S13
正常終了
正常終了を通知
エラーを返す
エラー

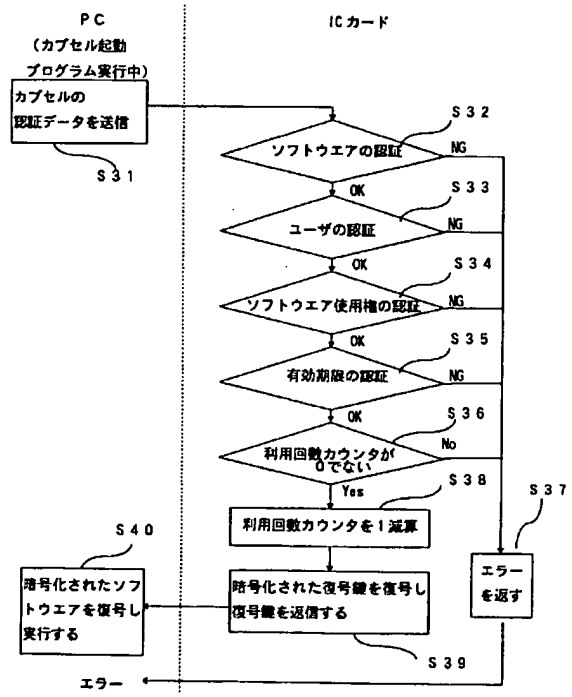
【図１０】



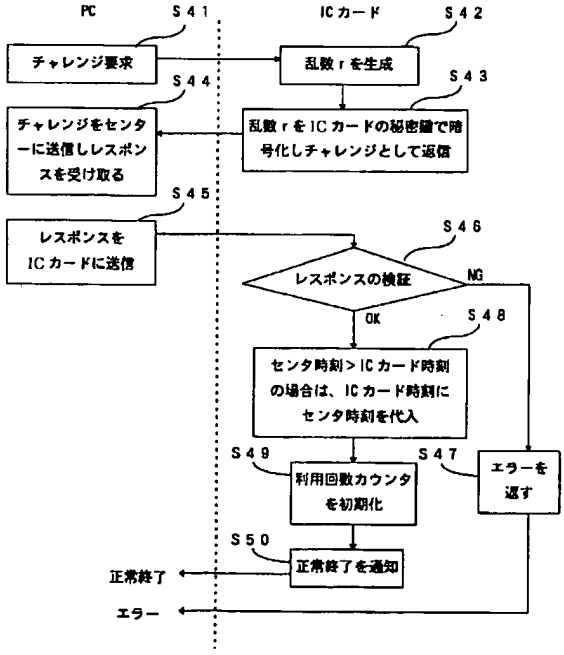
【図１２】



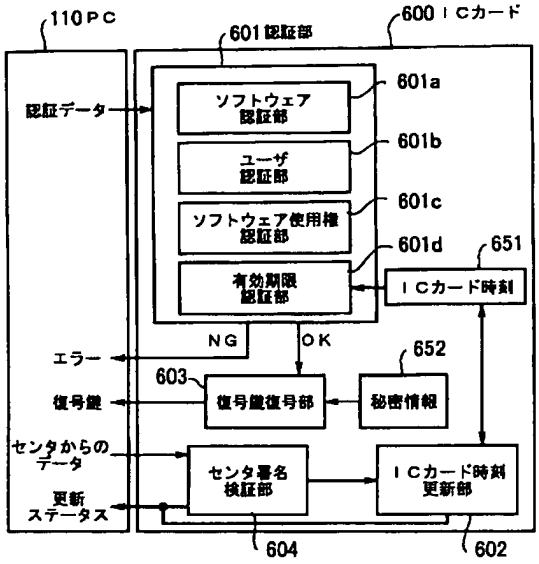
【図１３】



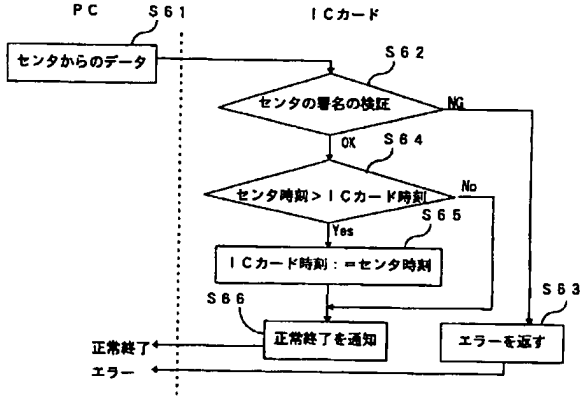
【図１４】



【図１５】



【図１７】



フロントページの続き

(72)発明者　千葉　健司
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

Ｆターム(参考)　5B085 AE02 AE03 AE06 AE12
5J104 AA07 AA11 MA01 PA10